Solution Brief

Secure and Protect DNS Traffic With DNS Over HTTPS (DoH)

Prevent Interference and Provide Privacy for DNS Queries for Overall Security

Security of the DNS infrastructure has never been more critical for service providers and for their enterprise customers. Many DDoS, ransomware and data theft attacks are carried out by targeting DNS. This is largely possible because the DNS query— the request between the DNS client and the local DNS server that provides the internet address— is transmitted in clear text, that is, unencrypted. Other sensitive user information such as passwords, credit card information, email addresses, etc. is usually transmitted over secure HTTPS protocol. This has not been the case for the DNS query. As a result, DNS queries are easily subject to spoofing, interception, hijacking and other issues.

To overcome this vulnerability, DoH has been proposed by the IETF, providing the DNS query the encryption protection of HTTPS. Several companies such as Microsoft, Google, Cloudflare, and Chromium and Mozilla offer or have announced it will support this capability.

A10 Networks offers DoH natively in its Thunder CFW for those organizations, typically service providers, that want to offer this capability to their subscribers. As demonstrated by service provider production use, the solution can handle the scale and new requirements DoH brings. The capability supports the high performance and low latency needed in DNS infrastructure while providing the encryption protection for DNS messages. This solution brief provides a summary of the benefits of DoH, as well as an overview of the DoH capabilities provided by A10 Networks.

This solution brief provides a summary of the benefits of DoH, as well as an overview of the DoH capabilities provided by A10 Networks.

Challenge

DoH potentially mitigates long-standing DNS vulnerabilities and provides deeper protection to subscribers against DNS-based attacks. However, in service provider networks DoH can disrupt many valued subscriber services, impair network performance and reduce operator control of subscriber experience

Solution

As a native function of A10 Networks Thunder CFW, DoH can be combined with DNS security features of the secure application service suite to support complete protection for DNS queries while maintaining the performance needed in service provider-scale DNS infrastructure,

Benefits

With DoH from A10 Networks, cable companies, mobile operators and ISPs can offer a market-proven, carrier-scale solution to those subscribers that demand strong protection.

Challenge: Weighing the Pros and Cons of DoH

DoH Responds to Industry Concerns on DNS Vulnerability

DNS is the cornerstone of the internet and DNS infrastructure is arguably one of the most critical components for operators. It is designed to handle a large volume of queries and is often the target of multiple attacks. Resilient, high performance DNS infrastructure is essential to the proper functioning of service provider networks and the internet itself. All communication sessions over service provider networks begin with the initial request for the internet address. Yet, unlike user information such as credit cards, emails and passwords, which are encrypted using HTTPS, those DNS query/response transmissions are made in clear text – with no encryption. As a result, the DNS vector is exploited for a large number of DDoS, ransomware, malware and data theft attacks.

IETF has responded to growing concerns about DNS-related cyber-attacks with a proposed standard in RFC 8484 called DNS over HTTPS technology that encrypts the communication path between end devices and local DNS resolvers using the same protocol, HTTPS, as is now typically used for the privacy of user traffic. While providing higher security for DNS queries, the proposed technology also presents some challenges for service providers.

DNS Encryption Prevents Use of DNS for Many Valued Subscriber Services

Visibility of DNS queries enables service providers to offer many highly valued services such as anti-malware tools (blocking/detecting user access to malicious sites), parental controls and content filters, low-latency video content delivery, law enforcement inquiries, and self-service installations. Cable operators, mobile network operators, ISPs and other service providers may find many value-added services will "break" when subscribers use DoH by default. Mobile network performance may suffer from the added latency and overhead of DoH.

Thunder CFW with DNS Over HTTPS (DoH)

Offer Greater Protection to Subscribers and Retain Control Over DNS-Dependent Services

To retain control of DNS queries and the visibility of DNS information and to prevent accidental service disruption, mobile network operators, cable operators, ISPs and other service providers can add DoH to their DNS infrastructure with a market-proven, high-performance solution from A10 Networks. Tier-one operator tested and in production, the A10 solution supports billions of DNS queries. It allows service providers to offer this capability to those subscribers who request it using DoH, preventing interruption of their network DNS infrastructure and retaining control of DNS-dependent services. Our comprehensive DNS solution that includes capabilities like advanced DNS load balancing, caching and protection is deployed in worldwide service providers in both physical and virtual networks. DoH is an extension of the DNS solution, and is already deployed in tier-one operator networks, supporting billions of DNS queries. The A10 DoH solution allows service providers to offer this capability to those subscribers who request it, prevent interruption of their network DNS infrastructure and retain control of DNS-dependent services.

With A10 Networks DoH feature in Thunder CFW, service providers can offer their subscribers the option of higher security and enhanced privacy protection through end-to-end encryption for DNS queries. Service providers can protect their ability to offer value-added services that depend upon DNS information, such as anti-malware tools, localized video content delivery, filters such as parental controls and respond to law enforcement. This can further strengthen their subscriber relationship and prevent accidently "breaking" offered services from subscribers using alternative DNS providers.

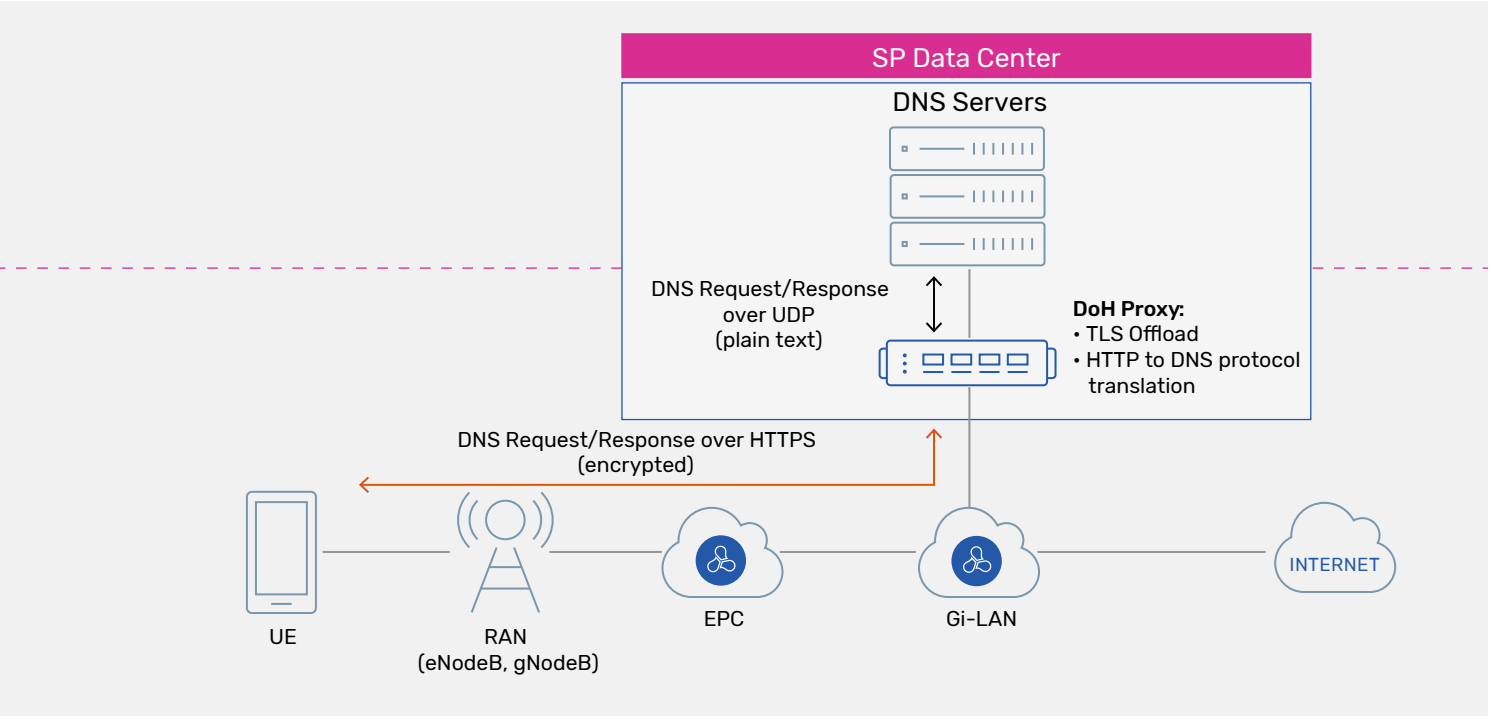

Figure 1: DNS over HTTPS in a mobile service provider network

Features and Benefits

DoH is available today as a native capability on any Thunder CFW appliance, hardware or software, enabling organizations to deploy any form factor they need. As a native function of A10 Networks Advanced Core Operating System (ACOS®), DoH can be combined with other security features of the Thunder CFW, including the application delivery controller (ADC) functionality to support comprehensive protection and availability for DNS, while maintaining the performance needed in service provider-scale DNS infrastructure.

Production proven at scale, Thunder CFW with DoH can support the low-latency expectations of service provider customers at millions of queries at peak and hundreds of billions of queries daily while provide user privacy and interference protection. The A10 solution is fully compliant with industry standards, RFC 8484/1035.

DoH Provides the Following Benefits:

Investment Protection: The Thunder CFW DoH capability is designed to protect and augment the existing DNS infrastructure investment for service providers. The existing DNS infrastructure solution components remain unchanged, and the secure connectivity and protocol translation are handled natively by Thunder CFW, which also includes multiple secure application services, including full application delivery controller functionality, as part of the A10 Orion 5G Security Suite.

Scale and Performance: The DoH encryption enabled by TLS requires additional processing capabilities. Thunder CFW is designed for the scale and performance required for high-volume DNS queries and DoH traffic. The encrypted DNS queries can be handled at scale by using built-in advanced hardware capabilities specifically designed to deal with encrypted sessions.

Security and Visibility: Thunder CFW provides secure application services to protect DNS infrastructure from multiple attack vectors. These are extended with the DoH capability. Organizations can combine multiple services as required, for example DNS Application firewall, DNS request and query rate limiting, DNS flood protection, DNS caching and more to improve the security, availability and performance of DNS infrastructure.

Solution Components

- Production-proven technology
- Native ACOS DoH and HTTP/2 Support
- Translates HTTP to DNS protocols
- Compliant with RFC 8484 and 1035
- Supports all DNS types and both IPv4 and IPv6 queries
- Currently deployed in operator networks, supporting millions of customers and billions of DNS queries
- Available with Thunder CFW
- Can be combined with network and security functions available on Thunder CFW

Quickly Enhance DNS Infrastructure with DoH

DNS over HTTPS is a proposed standard but is quickly gaining market traction due to strong support from web giants including Google and Mozilla. Service providers can rapidly add DoH functionality to existing DNS infrastructure without interrupting existing configurations. This will help retain service provider control over subscribers opting for DoH and prevent accidental "breaking" of value-added service that depend on DNS. Service providers can thus enhance the subscriber experience while providing added protection.

Next Steps

For more information, please visit www.a10networks.com/ products/thunder-cfw/.

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally. For more information, visit: a10networks.com and follow us @A10Networks

Learn More

About A10 Networks

Contact Us

a10networks.com/contact

Part Number: A10-SB-19207-EN-02 NOV 2020